ORACLE DATA SHEET

# Oracle Identity Governance Suite

ORACLE
FUSION MIDDLEWARE
IDENTITY MANAGEMENT

Organizations need to balance the requirements to provide users with quick access to the resources with the organization's risk and compliance obligation, ensuring that users only have access to the resources they need to perform their jobs. To achieve this balance, organizations need to deliver intuitive ways for users to request access to systems and applications, manage appropriate policies and processes to approve such access, provide simple ways for managers to confirm that such access is appropriate and finally, monitoring tools for managers and administrators to periodically check and certify that access is properly assigned to employees. Further, these systems need to apply to both standard user accounts and high risk, privileged accounts that are often shared by multiple administrators. Oracle provides a complete Identity Governance solution that enables organizations to efficiently balance the objectives of access, security, and compliance, while enabling user self-services to reduce total cost of ownership.

## KEY FEATURES

- Simplified, business friendly Self Service interface drives productivity and increases user satisfaction and operational efficiency
- Manage risk and reduce costs with a unified Identity Governance solution for both standard and privileged user access
- Choose a platform approach to Identity Management to see a 48% lower operational cost and 33% fewer audit deficiencies
- Centralized and extensible access catalog to store and further define business friendly definitions for Roles, Applications & Entitlements
- Simplified Access Requests with intuitive and flexible approval workflows and policy-driven provisioning improves IT efficiency, enhances security and enables compliance
- Role based access control with Role

## Oracle Identity Governance

Oracle Identity Governance reduces the total cost of ownership for organizations by empowering user self-service, simplifying audit and compliance tasks and automating IT operations. By delivering a comprehensive platform for access request, role lifecycle management, access certification, closed loop remediation and privileged account management, Oracle Identity Governance is a solution that address today's requirements and enables organizations to quickly adapt to emerging requirements. Oracle Identity Governance suite provides many benefits, including:

- Increased end user productivity – a business friendly and intuitive self-service experience that is both persona oriented and provides guided navigation, common business glossary for improved search, unified workflow orchestration and immediate access to key applications
- Increased IT productivity and automation of provisioning tasks, accelerated user-onboarding and stringent controls over sensitive access to shared privileged accounts
- Reduced total cost – single vendor platform for identity governance, combines comprehensive out-of-the-box capabilities with a flexible and simplified customization framework
- Reduced risk – guaranteed access revocation, detection and management of orphaned accounts, proactive and reactive IT audit policies (detection and enforcement), fine grained authorization controls and, continuous monitoring and role based access re-evaluation
- Increased efficiency – risk based identity certification on live data reduces overall time

ORACLE

Mining, Advanced Role Lifecycle Management and Role Analytics

- Risk-based, business user friendly Identity Certifications & closed loop remediation of access rights
- Continuous IT Audit Monitoring and Reporting to determine and take action on toxic combinations of access privileges across the enterprise

## KEY BENEFITS

- **Increased security:** Enforce internal security audit policies and eliminate potential security threats from rogue, expired and unauthorized accounts and privileges.
- **Privileged Account Management:** Allow authorized users to manage sensitive servers, applications and services in a controlled audited manner.
- **Enhanced regulatory compliance:** Cost-effectively enforce and attest to regulatory requirements (e.g. Sarbanes-Oxley, 21 CFR Part 11, Gramm-Leach-Bliley, HIPAA) associated with identifying who has access privileges to sensitive, high risk data
- **Improved business responsiveness:** Get users productive faster through immediate access to key applications and systems, while enforcing security policies
- **Reduced costs:** Reduce IT costs through efficient, business friendly self-service and platform-based architecture

## ARCHITECTURE OVERVIEW

- **Converged Solutions:** Oracle Identity Governance Suite solutions - Oracle Identity Manager, Oracle Identity Analytics & Oracle Privileged Account Manager work together to create a complete governance process for the enterprise
- **Ease of Deployment:** UI Customizations and integrations are durable and can survive patching and upgrades
- **Flexible and Resilient:** Oracle Identity Governance can be deployed in single or multiple server instances. Multiple server instances provide optimal configuration options, fault tolerance, redundancy, fail-over and

to certify access. Provisioning automation and closed-loop remediation ensure access is controlled and maintained.

### Business Friendly Self Service and Access Request

Organizations are eager to reduce costs and accelerate processes by empowering user self-service. Embracing this paradigm, Oracle Identity Governance solutions include out-of-the-box, business persona oriented self-service and guided navigation that enables end users to complete tasks seamlessly, while using a UI that is tablet friendly and pertains to the Identity Governance tasks they care about the most. In addition, Shopping cart style access request interfaces are designed to follow common practices popular on commercial e-commerce sites, such as “add to cart”, “review cart”, “checkout out” etc. Core to empowering end user self-service is the expressive Access Catalog: a glossary that includes user-friendly names for all systems and resources to simply the user process of searching for the right system or business application. Further, this catalog also includes enterprise items such as sensitive, privileged accounts, roles and entitlements, necessary to drive roles-based provisioning.

### Advanced Role Lifecycle Management

In an effort to effectively manage the proliferating number of users, many organizations are leveraging roles to assign and manage rights and privileges. To support this approach, Oracle Identity Governance includes innovative and robust role discovery and lifecycle management capabilities, which both harvest roles as they are created and manage approval processes for any changes to roles on an ongoing basis. In addition, robust Role Analytics enable role designers and approvers to evaluate the impact of role changes, with inline SoD violations checks, impacts to users and entitlements and metrics that help with role consolidation. All role activities are fully audited and changes can be rolled back if necessary.

### Streamlined Access Grants

While a business friendly interface simplifies the access request process, access grants must be approved by authorized entities, which may require various levels of information as justification for the request. Oracle Identity Governance leverages standards-based approval workflows, which include enterprise capabilities such as delegating approval and including supporting attachments on workflow requests to provide the additional detail required to make an approval decision.

### Simplified Identity Certification

As the number of applications to which employees have access increases, certifying access becomes imperative, especially for larger enterprise organizations. In order to efficiently scale and sustain, these processes need to be both automated and resilient. With advanced, risk-based analytics and easy to navigate dashboards, Oracle Identity Governance offers a robust set of identity certification features that streamline the review and approval processes to effectively manage risk on an ongoing basis. Beyond understanding “who has access to what”, in depth analytics can provide detailed graphical and actionable business context, as well as 360-degree views on how such access was granted and highlights outliers for individuals versus their roles. In addition, Identity Certifications promote business user friendliness via innovative capabilities such as the ability for reviewers to complete certifications offline. In addition, workflow capabilities that allow both Business and IT teams to collaborate on a single Identity

system load balancing

- **Maximum Reuse of Incumbent Infrastructure:** Oracle Identity Governance is built on an open architecture to integrate with and leverage existing software and middleware already implemented within an organization's IT infrastructure
- **Standards-based:** Oracle Identity Governance incorporates leading industry standards, such as J2EE, BPEL and OASIS

**AVAILABLE CONNECTORS**

- **Business Applications:** Oracle Fusion Applications, Oracle E-Business, PeopleSoft, JD Edwards, Siebel and SAP
- **LDAP stores:** Oracle Internet Directory, Oracle DSEE, Oracle Unified Directory, Active Directory and e-Directory
- **Security systems:** RSA, RACF, Top Secret, ACF2
- **Collaboration Suites:** Exchange/Domino and GroupWise
- **Operating systems:** OEL, Red Hat Linux, HP-UX, AIX, Solarix, AS/400 and Windows
- **Ticket Management systems:** BMC Remedy
- **Cloud Connectors:** Oracle CRM On-demand, Google Apps
- **Databases: Oracle,** MySQL, SQL Server, DB2, Sybase
- **Technology Integrations:** SSH, Telnet, Flat File, JDBC, LDAP V3, SOAP, REST

Certification campaign are also included. Finally, the solution offers closed loop remediation, which provides an automated way for reviewers to revoking improper access across target systems and includes alerts should remediation fail.

## Privileged Account Management

Within virtually every organization, there are sensitive, privileged accounts, such as Root Admin accounts. These accounts must be shared between multiple users and are frequently managed insecurely. Oracle identity Governance enables organizations to extend core identity management policies to these sensitive, privileged accounts. Administrators, or super users seeking access to these accounts can use the standard, access request interface and Access Catalogue to request access to these privileged accounts. Standard approval workflows and certifications apply and organizations can leverage their existing Oracle Identity Manager connectors to manage the privilege account passwords.

## IT Audit Monitoring & Reporting

Oracle identity Governance provides both policy-based audit monitoring and detailed and flexible reporting capabilities. Comprehensive dashboards enable both system administrators and delegated administrators to run reports on virtually any artifact of a user's access rights, access grants and the genesis of each. The Oracle Identity Governance Suite offers the ability to define and enforce detailed security policies both within and across applications to enforce continuous Segregation of Duties analysis. This enables intelligent monitoring and to identify and remediate imminent violations typically caused by access grants following job changes or other HR events. Finally, decisions made to identity certification reports are always stored and archived for audit purposes.

ORACLE

CONTACT US

For more information about Oracle Identity Governance visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

**Hardware and Software, Engineered to Work Together**